UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/745,808	12/26/2000	Masayuki Terao	Q62445	2609

7590 07/13/2005

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037

EXAMINER	
CHAI, LONGBIT	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/745,808	TERAO ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *6-11* is/are pending in the application.

4a) Of the above claim(s) *1-5,12-23,25,26,28-31,33 and 34* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *6-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's election of Group II filed on 6/3/2005 with respect to restriction requirement mailed on 3/3/2005 from the following three groups is acknowledged and accordingly, this Office Action only addresses the claimed inventions of Group II as elected by Applicant.

This application contains claims directed to the following patentably distinct claimed inventions. Restriction to one of the following invention is required under 35 U.S.C 121:

I. Claims 1 – 5 and 12 – 19 drawn to the overall computer / network security system, in general, classified in class 713, subclass 200.

II. Claims 6 – 11 drawn to mutual entity authentication in a computer security system, classified in class 713, subclass 169.

III. Claims 20 – 23, 25 – 26, 28 – 31 and 33 – 34 drawn to user-to-user key distributed over data link in a computer / network security system, classified in class 380, subclass 283.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Koike (Patent Number: 6243578), in view of Quick (Patent Number: 6178506), and in view of Clark (Publication Number: 2001/0011308).

As per claim 6, Koike teaches a method of conducting authentication between a communication device which can be freely inserted into and extracted from a slot of a terminal device and said terminal device (Koike: see for example, Figure 1), comprising the steps of:

Koike does not disclose expressly (a) inserting a key module storing the same ID as an ID stored in the communication device into the slot to register the ID stored in the key module at the terminal device, and (b) conducting collation between the terminal device and the communication device inserted into the slot to determine whether the ID stored in the communication device and the ID registered at the terminal device coincide with each other.

Quick teaches inserting a key module to register the ID stored in the key module at the terminal device (Quick: see for example, Column 1 Line 53 – 65).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Quick within the system of Koike in view of Shigeki because Quick teaches providing the user registration information through the use of an inserted module with interface adaptable to the terminal device (Quick: see for example, Column 1 Line 59 – 65).

Koike in view of Quick does not disclose expressly the key module storing the same ID as an ID stored in the communication device.

Clark teaches the key module storing the same ID as an ID stored in the communication device (Clark: see for example, Paragraph [0010] Page 2 Line 9 – 12 an Paragraph [0060] Page 8 Line 6 – 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Clark within the system of Koike in view Quick because Clark teaches providing an effective mechanism, i.e. registration serial number, to synchronize between the host computer and a cradle assembly connected to the host computer (Clark: see for example, Paragraph [0010] Page 2 Line 9 – 12 an Paragraph [0060] Page 8 Line 6 – 9).

Accordingly, Koike in view Quick and Clark teaches (a) inserting a key module storing the same ID as an ID stored in the communication device into the slot to register the ID stored in the key module at the terminal device, and (b) conducting collation between the terminal device and the communication device inserted into the slot to determine whether the ID stored in the communication device and the ID registered at the terminal device coincide with each other.

3. Claims 7 – 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koike (Patent Number: 6243578), in view of Quick (Patent Number: 6178506), in view of Clark (Publication Number: 2001/0011308), and in view of de la Huerga (Patent Number: 5960085).

As per claim 7, Koike in view of Quick and Clark teaches the claimed invention as described above (see claim 6). Koike in view of Quick and Clark does not teach when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted.

de la Huerga teaches when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted (de la Huerga: see for example, Column 4 Line 40 – 67 and Column 5 Line 1 – 11: de la Huerga teaches a security system equipped with a wireless device to exchange authentication information with the security badge of a system user (de la Huerga: see for example, Column 4 Line 42 – 43). After the authentication and system in service, the computer terminal continues to monitor the signal path between the security badge and the computer terminal. If the system user turns away from the computer terminal, then the keyboard is locked and the screen is blanked off (de la Huerga: see for example, Column 5 Line 3 – 5).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of de la Huerga within the system of Koike in view of Quick and Clark because de la Huerga teaches a limited access system for restricting and monitoring between wireless smart devices.

As per claim 8, Koike in view of Quick and Clark teaches the claimed invention as described above (see claim 6). Koike in view of Quick and Clark does not teach when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted.

de la Huerga teaches when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted (de la Huerga: see for example, Column 4 Line 40 – 67 and Column 5 Line 1 – 11).

Koike in view of Quick and Clark does not teach when the communication device is inserted into the slot of the locked terminal device to obtain authentication between the terminal device and the communication device, releasing the terminal device from the locked state.

de la Huerga teaches when the communication device is inserted into the slot of the locked terminal device to obtain authentication between the terminal device and the communication device, releasing the terminal device from the locked state (de la

Huerga: see for example, Column 4 Line 40 – 67 and Column 5 Line 10 – 11: de la Huerga teaches if the security badge is not properly positioned for more than a preset period of time, the system user will be logged off automatically. This implies the system user needs to go through the authentication process again after returning back to the proper position).

Same rational for combination applies here as above in rejecting the claim 7.

As per claim 10 and 11, claim 10 and 11 do not further teach over claim 7 and 8 respectively. Therefore, see same rationale addressed above in rejecting claim 7 and claim 8.

4. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Koike (Patent Number: 6243578), in view of Quick (Patent Number: 6178506), in view of Clark (Publication Number: 2001/0011308), and in view of Kung (Publication Number: 5434918).

As per claim 9, Koike teaches a method of conducting authentication between a communication device which can be freely inserted into and extracted from a slot of a terminal device and said terminal device (Koike: see for example, Figure 1), comprising the steps of:

Koike does not disclose expressly (a) inserting a key module storing the same ID and authentication code as an ID and an authentication code stored in the

communication device and storing a cryptographic function paired with an inverse cryptographic function stored in the communication device into the slot to register the ID, the authentication code and the cryptographic function stored in the key module at the terminal device,and (b) when the communication device is inserted into the slot, conducting authentication between the communication device and the terminal device, said step (b) including: (b-1) collating the ID stored in the communication device and the ID registered at the terminal device.

Quick teaches (a) inserting a key module storing the same ID and authentication code as an ID and an authentication code stored in the communication device and storing a cryptographic function paired with an inverse cryptographic function stored in the communication device into the slot to register the ID, the authentication code and the cryptographic function stored in the key module at the terminal device, and (b) when the communication device is inserted into the slot, conducting authentication between the communication device and the terminal device, said step (b) including: (b-1) collating the ID stored in the communication device and the ID registered at the terminal device (Quick: see for example, Column 1 Line 53 – 65 and Column 2 Line 55 – 57: Quick teaches using a key module to establish the user registration information and it is also well known in the field that registration information during the subscription time includes the user identity, initial subscription key Ki and the associated A3 cryptographic function).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Quick within the system of Koike in view

of Shigeki because Quick teaches providing the user registration information through the use of an inserted module with interface adaptable to the terminal device (Quick: see for example, Column 1 Line 59 – 65).

Koike in view of Quick does not disclose expressly the key module storing the same ID as an ID stored in the communication device.

Clark teaches the key module storing the same ID as an ID stored in the communication device (Clark: see for example, Paragraph [0010] Page 2 Line 9 – 12 an Paragraph [0060] Page 8 Line 6 – 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Clark within the system of Koike in view Quick because Clark teaches providing an effective mechanism, i.e. registration serial number, to synchronize between the host computer and a cradle assembly connected to the host computer (Clark: see for example, Paragraph [0010] Page 2 Line 9 – 12 an Paragraph [0060] Page 8 Line 6 – 9).

Accordingly, Koike in view Quick and Clark teaches (a) inserting a key module storing the same ID and authentication code as an ID and an authentication code stored in the communication device and storing a cryptographic function paired with an inverse cryptographic function stored in the communication device into the slot to register the ID, the authentication code and the cryptographic function stored in the key module at the terminal device, and (b) when the communication device is inserted into the slot, conducting authentication between the communication device and the terminal device,

said step (b) including: (b-1) collating the ID stored in the communication device and the ID registered at the terminal device.

Koike in view Quick and Clark does not disclose expressly (b-2) when collation of IDs succeeds, generating a random number, sending data obtained by encrypting the random number with the authentication code connected by the cryptographic function from the terminal device to the communication device and at the communication device side, restoring the authentication code and the random number by the inverse cryptographic function to collate the restored authentication code and the stored authentication code, and (b-3) when collation of authentication codes succeeds, sending data obtained by encrypting said restored random number by the inverse cryptographic function from the communication device to the terminal device and at the terminal device, restoring the random number by the cryptographic function to collate the restored random number with said random number generated by the own terminal device.

Kung teaches:

(b-2) when collation of IDs succeeds, generating a random number, sending data obtained by encrypting the random number with the authentication code connected by the cryptographic function from the terminal device to the communication device and at the communication device side, restoring the authentication code and the random number by the inverse cryptographic function to collate the restored authentication code and the stored authentication code (Kung: see for example, Column 4 Line 24 – 43: The Server as taught by Kung is equivalent to the terminal device and the Client is

equivalent to the communication device. The password is equivalent to the authentication code. The encrypted password is decrypted by the client and thereby authenticate the Server to the Client because the password is known to the user (Kung: see for example, Column 4 Line 24 – 27)), and

(b-3) when collation of authentication codes succeeds, sending data obtained by encrypting said restored random number by the inverse cryptographic function from the communication device to the terminal device and at the terminal device, restoring the random number by the cryptographic function to collate the restored random number with said random number generated by the own terminal device (Kung: see for example, Column 4 Line 44 – 51: The Server as taught by Kung is equivalent to the terminal device and the Client is equivalent to the communication device. The password is equivalent to the authentication code. Kung also teaches, after authenticate the Server to the Client, the Client transmitting an encrypted message using the random number, where the random number can also be used as the encryption / decryption key. The Server decrypting the encrypted message and thereby authenticate the Client to the Server because the random number is known to and originated by the Server (Kung: see for example, Column 4 Line 50 – 51).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kung within the system of Koike in view of Quick and Swamy because Kung teaches enhancing the system security by using mutual authentication between the Server and the Client (Kung: see for example, Column 1 Line 37 – 44).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100